ISSN 2500-1442

Научная статья
УДК 343
EDN ZOTPWX
DOI 10.17150/2500-4255.2026.20(5).541-551

ПРАВОВАЯ ГЕОПОЛИТИКА ЦИФРОВЫХ ТЕХНОЛОГИЙ И ТРАНСФОРМАЦИЯ ЦИФРОВОЙ ПРЕСТУПНОСТИ: ЭКСПЕРТНОЕ ИНТЕРВЬЮ С В.С. ОВЧИНСКИМ

Э.Л. Сидоренко
Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, г. Москва, Российская Федерация

Информация о статье

Дата поступления
25 сентября 2026 г.

Дата принятия к публикации
26 октября 2026 г.

Дата онлайн-размещения
25 ноября 2026 г.

Ключевые слова

Цифровая геополитика; правовая геополитика; цифровой суверенитет; киберпреступность; организованная преступность; искусственный интеллект; кибербезопасность; Вьетнам; Венесуэла; БРИКС

Финансирование

Статья подготовлена по государственному заданию МИД России. Соглашение о предоставлении субсидии от 30.01.2026 No. 310-03-2026-002 в рамках направления «Научно-технологическая политика незападных государств»

Аннотация. В статье в редком для академической периодики жанре экспертного интервью с советником министра внутренних дел Российской Федерации, доктором юридических наук, профессором В.С. Овчинским исследуется прямая зависимость между правовой геополитикой цифровых технологий и трансформацией цифровой преступности. Актуальность работы определяется тем, что межгосударственная борьба за контроль над вычислительными мощностями, искусственным интеллектом, квантовыми разработками, платформами и цифровыми финансами ведется сегодня прежде всего правовыми средствами — через экспорт технических стандартов, расширение национальной юрисдикции, режимы локализации данных и санкционные ограничения. Каждое такое изменение правовой архитектуры цифровой среды неизбежно перестраивает и криминальный рынок, открывая новые трансграничные ниши для киберпреступности. Методологически исследование построено как научный диалог двух криминологов, в котором оценки эксперта сопоставляются с данными международных индексов, аналитических докладов и новейших публикаций, получая системную правовую интерпретацию и прогностическое развитие. Доказывается, что правовая геополитика выступает стратегией навязывания правил цифровой среды, тогда как цифровой суверенитет является защитной реакцией государства; при этом наряду с государствами и транснациональными платформами самостоятельными участниками цифровой среды выступают преступные сети, использующие расхождения национальных юрисдикций. На материале отношений России с Китаем, Вьетнамом и Венесуэлой показано, что главным российским ресурсом в международном цифровом обмене является опыт обеспечения кибербезопасности и расследования ИТ-преступлений, однако его востребованность и защищенность от криминализации напрямую зависят от прочности государственных и правовых институтов страны-партнера. Сформулированы сценарии развития цифровой среды до 2030 г. и четыре ключевые криминологические угрозы ближайшего периода (отложенный квантовый взлом, криминальное применение искусственного интеллекта и «дипфейков», отмывание преступных доходов через криптоактивы, коммерциализация киберпреступности по сервисной модели). Сделаны выводы о необходимости предварительной криминологической оценки зарубежных цифровых проектов России как с системными партнерами (Китай, Вьетнам), так и со странами с высокой институциональной уязвимостью, а также о формировании на стыке международного права и криминологии самостоятельного направления, изучающего влияние правовых режимов цифровой среды на динамику преступности.

Для цитирования. Сидоренко Э.Л. Правовая геополитика цифровых технологий и трансформация цифровой преступности: экспертное интервью с В.С. Овчинским / Э.Л. Сидоренко. — DOI 10.17150/2500-4255.2026.20(5).541-551. — EDN ZOTPWX // Всероссийский криминологический журнал. — 2026. — Т. 20, № 5. — С. 541–551.

© Сидоренко Э.Л., 2026

ISSN 2500-1442

Original article

LEGAL GEOPOLITICS OF DIGITAL TECHNOLOGIES AND THE TRANSFORMATION OF DIGITAL CRIME: AN EXPERT INTERVIEW WITH V.S. OVCHINSKY

Elina L. Sidorenko
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, Moscow, the Russian Federation

Article info

Received
2026 September 25

Accepted
2026 October 26

Available online
2026 November 25

Keywords

Digital geopolitics; legal geopolitics; digital sovereignty; cybercrime; organized crime; artificial intelligence; cybersecurity; Vietnam; Venezuela; BRICS

Acknowledgements

The article was prepared in accordance with the state assignment of the Russian Ministry of Foreign Affairs. Agreement on the provision of a subsidy dated 30.01.2026 No. 310-03-2026-002 within the framework of the direction "Scientific and Technological Policy of Non-Western States"

Abstract. Written in the genre of an expert interview with Adviser to the Minister of Internal Affairs of the Russian Federation, Doctor of Law, Professor V.S. Ovchinsky — a format rarely used in academic journals — the article examines the direct link between the legal geopolitics of digital technologies and the transformation of digital crime. The relevance of the study stems from the fact that interstate competition for control over computing power, artificial intelligence, quantum technologies, digital platforms and financial channels is increasingly waged through legal instruments: export of technical standards, extraterritorial jurisdiction, data localization regimes and sanctions. Every shift in this legal architecture reshapes the criminal market and creates new cross-border niches for cybercrime. Methodologically, the study is structured as a scholarly dialogue between two criminologists, in which the expert's assessments are tested against global criminological indices, international reports and recent research to provide systemic legal evaluation and forecasting. It is argued that legal geopolitics operates as a strategy of projecting rules onto the digital environment, whereas digital sovereignty represents a state's defensive response; alongside states and transnational platforms, criminal networks act as autonomous participants that exploit jurisdictional gaps. Drawing on case studies of Russia's relations with China, Vietnam and Venezuela, the article demonstrates that Russia's primary asset in international digital cooperation is its expertise in cybersecurity and cybercrime investigation, yet the effectiveness of such cooperation and its resilience against criminalization critically depend on the institutional strength of the partner state. The article outlines development scenarios up to 2030 and identifies four major criminological threats: deferred quantum decryption, criminal use of artificial intelligence and deepfakes, money laundering through crypto-assets, and the rise of the "crime-as-a-service" model. It is concluded that Russia's foreign digital initiatives — both with strategic partners such as China and Vietnam and with institutionally vulnerable states—require preliminary criminological assessment, and that an interdisciplinary field should be developed at the intersection of international law and criminology to measure how changes in digital legal regimes redistribute criminal opportunities.
For citation. Sidorenko E.L. Legal Geopolitics of Digital Technologies and the Transformation of Digital Crime: An Expert Interview with V.S. Ovchinsky. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2026, vol. 20, no. 5, pp. 541–551. (In Russian). EDN: ZOTPWX. DOI: 10.17150/2500-4255.2026.20(5).541-551.

Введение

Развитие цифровых технологий в последнее десятилетие не только трансформировало мировую экономику, но изменило и саму природу межгосударственного соперничества. Контроль над вычислительными мощностями, данными, платформами и стандартами искусственного интеллекта (далее — ИИ) превратился в самостоятельное измерение геополитики, а правовые инструменты (юрисдикция, техническое нормирование, режимы трансграничной передачи данных, санкционные механизмы) стали средствами стратегического противоборства. Данный процесс можно обозначить понятием «правовая геополитика цифровых технологий».

Для криминологии наблюдаемая цифровая и следующая за ней правовая трансформация имеют принципиальное значение. Правовая архитектура цифровой среды задает не только поле легальной технологической конкуренции, но и структуру криминальных возможностей: преступность проникает в те зоны, где правовые режимы расходятся, ослабевают либо используются как инструмент давления. В отечественной науке сформирован прочный фундамент для анализа этой проблематики — от исследований мировых и российских тенденций преступности [1, с. 65] и первых работ, посвященных информационным компьютерным преступлениям [2], до осмысления киберпреступности как новой

криминальной угрозы [3, с. 47] и становления криминологии цифрового мира как самостоятельного направления [4]. Вместе с тем анализ отечественных и зарубежных исследований показал, что связь между геополитической борьбой за цифровые правила и трансформацией цифровой преступности до настоящего времени не получила системного освещения. Большинство работ посвящено либо международно-политическим аспектам технологического соперничества, либо отдельным видам киберпреступлений, тогда как их взаимная обусловленность, в особенности применительно к зарубежным партнерствам России в Азиатско-Тихоокеанском регионе и Латинской Америке, остается недостаточно изученной.

В этой связи цель настоящей статьи — выявить связь между правовой геополитикой цифровых технологий и трансформацией цифровой преступности, а также определить место России в формирующейся архитектуре цифровой безопасности. Для ее достижения последовательно решаются следующие задачи: уточняется содержание категории «цифровая геополитика» и ее соотношение с цифровым суверенитетом; определяется круг акторов, включая транснациональные платформы и преступные сети; оценивается характер российско-китайского технологического партнерства; сопоставляются вьетнамский и венесуэльский векторы российской цифровой политики; формулируются сценарии развития до 2030 г., ключевые криминологические угрозы и индикаторы их различения.

Методология исследования

Методологическую основу исследования составил метод экспертного интервью, дополненный системным, сравнительно-правовым и прогностическим методами. Экспертом выступил доктор юридических наук, профессор, заслуженный юрист Российской Федерации В.С. Овчинский, на протяжении нескольких десятилетий исследующий организованную преступность и ее цифровую трансформацию [4; 5]. Беседа проведена профессором Э.Л. Сидоренко в октябре 2026 г. по сценарию, включавшему шесть тематических блоков; расшифровка интервью научно отредактирована и согласована с экспертом. Позиции эксперта не принимались как данность, а рассматривались в качестве исследовательских гипотез, подлежащих проверке на материале научных публикаций, докладов международных организаций и данных глобальных криминологических мониторингов. Сравнительный метод позволил сопоставить российско-вьетнамский и российско-венесуэльский векторы как кейсы эффективности и пределов цифрового сотрудничества, системный подход — выявить взаимосвязь инфраструктурного, нормативного и криминального уровней цифровой среды, а сценарный анализ — сформулировать проверяемые прогнозы на горизонт 2030 г.

Основные результаты исследования

Цифровая геополитика как правовая и криминологическая категория. Исходный вопрос исследования состоит в том, является ли «цифровая геополитика» самостоятельной правовой и криминологической категорией или лишь метафорой классической борьбы за ресурсы в информационной среде.

По оценке В.С. Овчинского, это «осязаемая реальность с конкретным политическим наполнением», где «война ведется не столько войсками, сколько данными, алгоритмами и каналами информации». На вершину иерархии объектов борьбы эксперт ставит ИИ в его движении к общему искусственному интеллекту, далее — квантовые вычисления, «обессмысливающие значительную часть действующих систем криптографической защиты», затем платформы как «инфраструктуру управления глобальным вниманием» и криптоактивы как органическую часть цифровой экономики, причем в США происходит прямое сращивание технологических корпораций с военным ведомством [4; 5]. Принципиально важно, что эта иерархия зеркально воспроизводится в криминальной среде: те же алгоритмы, уязвимости шифрования, платформенные экосистемы и криптовалютные контуры образуют инфраструктуру транснациональной киберпреступности.

Механизм этой связки раскрывают Г. Фаррелл и А. Ньюман: государство, контролирующее узловые точки глобальных сетей, превращает взаимозависимость в инструмент принуждения — от санкций до отключения от финансовой и информационной инфраструктуры [6, с. 42]. В отечественной доктрине такое противоборство обоснованно рассматривается как новая форма межгосударственного конфликта [7]. Криминологическое следствие состоит в том, что санкционная фрагментация и отключение от легальных расчетов не устраняют трансграничные потоки, а вытесняют их в непрозрачные юрисдикции и теневые платежные контуры, институционализируя криминальные рынки.

В правовой геополитике цифровых технологий выделяются три уровня: инфраструктурный (контроль над узлами сетей и вычислениями), нормативный (экстерриториальная юрисдикция, режимы данных, техническое нормирование, экспансия которых, по С. Хоффманн и соавторам, ведет к фрагментации сети на несовместимые сегменты [8, с. 239]) и доктринальный, связанный с категорией цифрового суверенитета, которую Дж. Поле и Т. Тиль характеризуют как «концепт-зонтик» с различным наполнением в европейской, китайской и российской моделях [9]. Если правовая геополитика — это наступательная стратегия закрепления технологической ренты через экспорт собственных норм и стандартов, то цифровой суверенитет — защитная правовая реакция государства; при этом конкуренция в сфере ИИ развивается как «геополитическая инновационная гонка», в которой самоизоляция снижает потенциал участника [10, с. 1907].

Отсюда следует ключевой криминологический вывод: правовая архитектура цифровой среды прямо детерминирует структуру криминальных возможностей. Коллизии национальных юрисдикций, расщепление стандартов и свертывание правоохранительного сотрудничества создают зоны правового вакуума и «юрисдикционного арбитража», которые заполняют транснациональные преступные сети. Поэтому сдвиги в правовой геополитике выступают прямым криминогенным фактором цифровой преступности.

Акторы цифровой геополитики и стратегии кибербезопасности. Определение предмета цифровой геополитики ставит вопрос о субъектах, которые формируют правовой режим цифровой среды и тем самым задают границы криминальной активности. В.С. Овчинский фиксирует многослойность акторов: государства пытаются «задать правила», однако фактическими держателями инфраструктуры стали транснациональные платформы, социальные сети, облачные провайдеры и операторы спутниковых группировок. В США сложился симбиоз дерегулирования ИТ-корпораций в обмен на лояльность и выполнение квазигосударственных, в том числе военно-разведывательных, функций; в Китае государство удерживает вертикаль управления технологиями и кадрами, компенсируя демографический спад роботизацией. Третий контур образуют страны «глобального Юга», по выражению эксперта, — «качающийся электорат» цифровых блоков, за привязку которого США конкурируют платным доступом к передовым системам, а Китай — бесплатным распространением дистиллированных моделей и инфраструктуры.

Правовое следствие этой многослойности — размывание государственной монополии на юрисдикцию и принуждение. Платформы превратились в «частных регуляторов», чьи алгоритмы и регламенты выдачи данных фактически определяют успех расследования киберпреступлений. При этом китайская модель также ушла от жесткого администрирования к гибкой координации государства, индустрии и науки, как показывают С. Фу и Т. Хуан [11], а внешнюю экспансию, по данным М. Кантеро Гамито, Пекин ведет через продвижение технических стандартов ИИ в международных органах стандартизации, конвертируя техническое нормирование в геополитическое влияние [12].

В эту же архитектуру встраивается еще один слой акторов — транснациональные преступные сети. Как показали Э. Лукфельдт и соавторы, цифровая организованная преступность соединяет «безграничные возможности» киберпространства с глубокой локальной укорененностью (вербовкой исполнителей, социальными связями и территориальными каналами легализации доходов) [13, с. 324]. Используя несовместимость американской и китайской юрисдикций и отсутствие универсального обмена цифровыми доказательствами, криминальные структуры разносят управление, жертв и финансовые шлюзы по разным правовым контурам. Тем самым платформы и стандарты формируют не только геополитический, но и криминальный порядки.

Для стран «глобального Юга» и объединений вроде БРИКС, рассматривающих кооперацию в сфере ИИ как условие технологического суверенитета [14, с. 112], это создает прямой риск: импорт чужих платформ без адекватных механизмов правоохранительного контроля превращает их рынки в полигон киберпреступности. Отсюда следует прогноз: к 2030 г. борьба за развивающиеся государства сместится от поставок технологий к экспорту правовых режимов — правил локализации данных, платформенного надзора и процедур трансграничных киберрасследований.

Российско-китайское партнерство: взаимодополняющая асимметрия. Борьба сверхдержав за «глобальный Юг» напрямую ставит вопрос о месте России в новой правовой архитектуре цифровой среды. Москва и Пекин

совместно выдвигают инициативу Всемирной организации по ИИ с равным доступом развивающихся стран и решают сходные задачи — создание независимых технологических стеков, подготовку кадров и суверенное регулирование. Однако общность геополитических целей не означает равенства потенциалов.

По оценке В.С. Овчинского, российско-китайское партнерство «реальное, но асимметричное». Китай заинтересован в российской ядерной энергетике, фундаментальных научных школах и «зреющих идеях», прежде всего в квантовых технологиях, тогда как по вычислительным мощностям ИИ Россия уступает: «дата-центр без научной идеи — недвижимость, а не прорыв». Главным экспортным ресурсом страны эксперт называет кибербезопасность, востребованную на постсоветском пространстве и перенимаемую в БРИКС и ШОС. Опираясь на собственный опыт создания в МВД России подразделения по борьбе с киберпреступностью, он выделяет модель обмена данными об угрозах между правоохранительными органами и банками: «государство не может платить рыночные зарплаты, но может делиться информацией». В условиях блокировки западных рынков объединения БРИКС, ШОС и СНГ выступают для России «не идеологической, а жизненной необходимостью» [15].

Эта асимметрия проявляется в трех плоскостях. В доктринальной плоскости российский подход к международной информационной безопасности, как показывает А.А. Стрельцов, опирается на государственный суверенитет, юрисдикцию в ИКТ-среде и верховенство ООН [16, с. 87], тогда как китайская концепция киберсуверенитета сосредоточена на контроле внутреннего контента и платформ. Сближение этих позиций требует перехода от классических дипломатических деклараций к сетевым механизмам доверия [17, с. 325], международно-правовой базой которых выступает Конвенция ООН против киберпреступности[1], а теоретической — отечественная концепция международного управления Интернетом [18].

В криминологической плоскости позицию России осложняет двойственность: экспортируя передовые системы защиты, страна по данным рейтинга World Cybercrime Index одновременно входит в тройку мировых источников киберпреступных угроз [19], что снижает доверие к ее решениям на рынках БРИКС. Объяснить этот парадокс позволяет концепция А.И. Долговой, рассматривающая организованную преступность как устойчивую систему связей («криминальное общество»), использующую те же кадровые и интеллектуальные ресурсы, что и легальная среда [20, с. 7]. В цифровой сфере сильная инженерно-математическая традиция одновременно порождает и высококвалифицированную киберпреступность, и уникальную практику борьбы с ней. Именно этот правоохранительный и криптографический опыт компенсирует России нехватку вычислительных мощностей в диалоге с Пекином. Поэтому российско-китайское взаимодействие следует определять как взаимодополняющую асимметрию, а предлагаемая двумя странами Всемирная организация по ИИ будет жизнеспособна лишь тогда, когда выработает прикладные стандарты кибербезопасности и механизмы разрешения споров.

Вьетнам как пилотная площадка цифровой дипломатии России в АТР. Правоохранительная экспертиза как главный российский ресурс получает практическое воплощение прежде всего на вьетнамском направлении. Совместное заявление России и Вьетнама 2024 г. закрепило курс на кооперацию в цифровой сфере и взаимную правовую помощь по делам о преступлениях в сфере компьютерной информации[2]; в октябре 2026 г. в Москве прошла конференция по кибербезопасности с участием российских и вьетнамских специалистов[3], обсуждаются взаимное признание электронных подписей и трансграничный электронный документооборот.

В.С. Овчинский характеризует Вьетнам как «едва ли не самую перспективную страну» для российского сотрудничества. Принятый в стране план развития технологий, ИИ и робототехники до 2030 г. реализуется с опорой одновременно на Китай и США, а «бамбуковая дипломатия» Ханоя, по образному выражению эксперта, — это «гибкий ствол с прочными корнями». Вьетнаму необходимы технологические партнеры, Рос-

[1] United Nations Convention against Cybercrime: General Assembly Resolution A/RES/79/243 of 26 December 2024.

[2] Совместное заявление Российской Федерации и Социалистической Республики Вьетнам о дальнейшем развитии отношений всеобъемлющего стратегического партнерства (Ханой, 20 июня 2024 г.) // Президент России : офиц. сайт. URL: http://kremlin.ru/supplement/6157 (дата обращения: 20.10.2026).

[3] Эксперт Нгуен: Вьетнам и РФ могли бы объединить усилия в сфере кибербезопасности // ТАСС. 2026. 16 окт. URL: https://tass.ru/ekonomika/28224271 (дата обращения: 20.10.2026).

сии — вход в регион; при этом ограничения реальны: «Ханой никогда не пойдет на шаги, которые США или Китай прочтут как выбор стороны».

Высокий интерес России к вьетнамскому направлению объясняется тем, что цифровая трансформация Вьетнама развивается стремительными темпами, но при этом опережает возможности национальной системы киберзащиты. С одной стороны, налицо быстрый экономический рост, закрепленный в программных документах, — Национальной стратегии развития ИИ до 2030 г.[4] и партийной резолюции о научно-технологическом прорыве[5]: по итогам 2025 г. доля цифровой экономики в ВВП страны достигла 14 %[6], электронная коммерция стала одним из локомотивов внешней торговли [21, с. 95], а решения на базе ИИ активно используются для экономической интеграции в АСЕАН [22, с. 47].

С другой стороны, быстрое расширение цифрового рынка сделало страну мишенью для транснациональной организованной преступности, сформировавшей в Юго-Восточной Азии целую индустрию онлайн-мошенничества. Криминологические исследования показывают, что Вьетнам сталкивается с этой угрозой сразу в двух измерениях: внутри страны действуют разветвленные схемы компьютерного обмана и вывода похищенных средств, детально описанные Т. Ван Нгуен [23, с. 226], а за ее пределами граждане Вьетнама массово вовлекаются в работу зарубежных мошеннических центров («скам-кампусов»), где, как показали Х. Лыонг и Х. Нго, людей удерживают посредством обмана при трудоустройстве, изъятия документов и долговой кабалы [24; 25]. Именно эта потребность Ханоя защитить растущую цифровую экономику от криминального давления и делает востребованным российское предложение.

Сотрудничество здесь выстраивается на двух взаимодополняющих уровнях: взаимное признание электронных подписей и доверенный документооборот создают защищенные каналы для легальной внешней торговли, а объединение усилий в сфере кибербезопасности[7] и обмен оперативным опытом опираются на наработки отечественной криминологии и уголовно-правовой науки в области предупреждения компьютерных преступлений [26, с. 77; 27].

Венесуэла: пределы и риски стратегии цифрового сотрудничества. Если вьетнамский кейс демонстрирует условия эффективности цифрового партнерства, то венесуэльский позволяет установить его пределы. По оценке В.С. Овчинского, после смены власти в январе 2026 г. «о Венесуэле как объекте стратегической ставки нужно забыть»: новое руководство выстроило линию на сотрудничество с США, американские нефтяные компании восстановили позиции в экономике страны, а партнерство с Россией в этой конфигурации стало «фактором риска, а не ресурсом». Саму январскую операцию эксперт расценивает как геополитическое, а не криминологическое событие, а обвинения прежнего руководства в наркоторговле — как «пропагандистское оформление силового передела влияния», адресованное прежде всего Пекину.

Соглашаясь с практическим выводом эксперта, следует подчеркнуть аналитическую ценность данного кейса: он демонстрирует, что происходит с цифровой экономикой государства со слабыми институтами под экстремальным санкционным давлением. В Венесуэле сошлись три процесса. Во-первых, сложился режим «сотрудничества государства и преступности», при котором криминальные структуры встраиваются в государственные функции — от регулирования местных рынков до контроля приграничной ренты[8] [28, с. 599]. Во-вторых, кризис и санкции сместили источники богатства правящей элиты от нефтяной ренты к нелегальным товарам

[4] О национальной стратегии исследований, разработок и применения искусственного интеллекта до 2030 года : решение Правительства Социалист. Респ. Вьетнам от 26 янв. 2021 г. № 127/QĐ-TTg // LuatVietnam. URL: https://english.luatvietnam.vn/decision-no-127-qd-ttg-dated-january-26-2021-of-the-prime-minister-on-the-promulgation-of-the-national-strategy-on-research-development-and-applica-197755-doc1.html (дата обращения: 20.10.2026).

[5] О прорывах в развитии науки, технологий, инноваций и национальной цифровой трансформации : резолюция Политбюро ЦК Коммунист. партии Вьетнама от 22 дек. 2024 г. № 57-NQ/TW // Vietnam Law & Legal Forum. 2026. 7 июня. URL: https://vietnamlawmagazine.vn/novel-provisions-in-the-law-on-artificial-intelligence-and-recommendations-for-further-improvement-79932.html (дата обращения: 20.10.2026).

[6] Цифровая экономика на пороге нового этапа роста // Нянзан. 2026. 26 авг. URL: https://ru.nhandan.vn/tsifrovaja-ekonomika-na-poroge-novogo-etapa-rosta-post65681.html (дата обращения: 20.10.2026).

[7] Эксперт Нгуен: Вьетнам и РФ могли бы объединить усилия в сфере кибербезопасности.

[8] The Rise of the Criminal Hybrid State in Venezuela / InSight Crime. New York, 2023. 53 p. URL: https://insightcrime.org/wp-content/uploads/2023/07/Rise-of-the-Criminal-Hybrid-State-in-Venezuela-InSight-Crime-1.pdf (дата обращения: 20.10.2026).

и криптовалютным потокам, породив феномен «криптократов» [29, с. 1]. В-третьих, распространение криптоактивов в Латинской Америке обусловлено уязвимостью национальных финансовых систем — инфляцией, валютным контролем и санкционными ограничениями [30, с. 5].

При этом санкционная непрозрачность цифровых каналов представляет собой «палку о двух концах»: механизмы, обеспечивающие устойчивость к внешнему давлению, при отсутствии финансового контроля облегчают легализацию преступных доходов, что согласуется с выявленными типовыми схемами отмывания с использованием децентрализованных финансов [31, с. 822]. После январских событий 2026 г. международные мониторинги фиксируют дальнейшую фрагментацию криминального ландшафта страны и перераспределение контроля над наркотрафиком и золотом[9]. Обобщая, можно сформулировать модель цифровой криминализации: «цифровая инфраструктура устойчивости», построенная в обход международных правовых режимов на слабой институциональной базе, закономерно вырождается в криминальную инфраструктуру. Для российской стратегии из этого следует правило: криминологическая экспертиза институтов партнера по критерию «государственность/криминальность» должна предшествовать цифровым инвестициям.

Прогнозы и риски развития цифровой геополитики и стратегии кибербезопасности. Сопоставление вьетнамского и венесуэльского кейсов показывает, что успех цифровой стратегии определяется качеством правовой и институциональной среды. Это позволяет перейти к прогнозированию. Повестку новой цифровой геополитики можно свести к пяти вопросам: контроль над чипами и вычислениями, суверенные ИИ-стеки, управление данными, кибербезопасность критической инфраструктуры и правила применения ИИ в военной сфере. В.С. Овчинский поддерживает этот подход, расставляя акценты: контроль над вычислениями — это «вопрос вопросов», суверенные стеки отражают выбор между «платным и доминирующим» американским и «дистиллированным и бесплатным» китайским вариантами, а по военному ИИ «разговоров больше, чем правил». Ключевой тезис эксперта состоит в том, что Россия не проигрывает конкуренцию интеллектуально и при сохранении научных школ и экспорта кибербезопасности сохранит нишу, «которую не займет ни одна держава».

Прогнозы о полном распаде глобального Интернета на изолированные национальные сети («сплинтернет») представляются преувеличенными. Скорее формируется модель, в которой большинство стран, подобно Вьетнаму или Казахстану, не делают окончательного выбора в пользу США или Китая, а одновременно пользуются технологиями обоих центров силы. Поэтому водораздел проходит не по кабелям и оборудованию, а по правовым режимам: у каждой державы складываются собственные правила хранения данных, технические стандарты и пределы национальной юрисдикции[10].

В этих условиях положение России к 2030 г. может развиваться по одному из трех сценариев. Благоприятный сценарий предполагает, что страна сохранит инженерно-математические школы, добьется практических результатов в квантовых технологиях и закрепит за собой роль ведущего поставщика систем кибербезопасности для стран БРИКС и «глобального Юга». Инерционный сценарий означает сохранение технологического отставания в сфере вычислительных мощностей при удержании отдельных нишевых преимуществ. Наконец, кризисный сценарий связан с возможным обострением международных конфликтов вокруг Тайваня или Ближнего Востока, которое способно разрушить цепочки поставок микроэлектроники и привести к принудительному отключению целых регионов от глобальной инфраструктуры. Понять, по какому пути развивается ситуация, позволят три практических показателя: объем зарубежных контрактов российских компаний в сфере киберзащиты, динамика оттока либо возвращения ИТ-специалистов и темпы принятия единых цифровых стандартов внутри БРИКС.

Вне зависимости от того, какой сценарий реализуется, правоохранительной системе предстоит столкнуться с четырьмя взаимосвязанными угрозами.

Первая — квантовая: злоумышленники и спецслужбы уже сегодня накапливают зашифрованные массивы государственных, медицинских и банковских данных с расчетом вскрыть их через несколько лет, когда появятся достаточно мощ-

[9] What Are the Implications of the US Intervention in Venezuela for Organized Crime? // Global Initiative Against Transnational Organized Crime. Geneva, 2026. Jan. 6. URL: https://globalinitiative.net/analysis/what-are-the-implications-of-the-us-intervention-in-venezuela-for-organized-crime (дата обращения: 20.10.2026).

[10] What Are the Implications of the US Intervention in Venezuela for Organized Crime?

ные квантовые компьютеры, способные взломать современную криптографию [32]. Вторая угроза связана с развитием генеративного ИИ и технологией «дипфейков», которые не только удешевляют мошенничество и вымогательство, но и подрывают доверие к видео- и аудиозаписям как судебным доказательствам [33], что требует пересмотра подходов к уголовно-правовой оценке преступлений, совершаемых с применением ИИ [34; 35]. Третья угроза лежит в финансовой плоскости: по расчетам С. Фоли и соавторов, около 46 % транзакций с биткоином обслуживали теневой оборот [36, с. 1798], а российские исследования показывают, что при устойчивом росте криптопреступности [37, с. 85] суды и следствие до сих пор испытывают трудности при квалификации хищений цифровых активов [38, с. 18]. Четвертая угроза — перестройка самого криминального рынка по образцу легального ИТ-бизнеса, когда готовые инструменты взлома, фишинга и отмывания денег сдаются в аренду любому заказчику по модели «преступление как услуга» [39, с. 145]. Противостоять такой индустрии невозможно одними запретами — необходима работа на опережение с внедрением сопоставимых по уровню аналитических и прогнозных технологий в деятельность самих правоохранительных органов [40].

Заключение

Проведенное исследование позволяет сформулировать следующие выводы.

Правовая геополитика цифровых технологий представляет собой самостоятельное измерение межгосударственного соперничества за контроль над вычислительными мощностями, искусственным интеллектом, квантовыми разработками, платформами и цифровыми финансами. Если правовая геополитика выступает наступательной стратегией закрепления технологической ренты через экспорт национальных стандартов и экстерриториальной юрисдикции, то цифровой суверенитет — защитной правовой реакцией государства. При этом фрагментация глобальной сети развивается прежде всего не по техническому, а по нормативному контуру — через расхождение режимов локализации данных, стандартов и юрисдикций.

Состав субъектов этого противоборства утратил государственную монополию. Квазигосударственные функции регулирования коммуникаций и выдачи цифровых доказательств сосредоточили транснациональные платформы, а возникающие коллизии национальных юрисдикций и отказ от обмена правоохранительными данными осваивают транснациональные преступные сети. В результате правовая геополитика и цифровая преступность функционируют как взаимосвязанные процессы: архитектура правовых и технических норм одновременно определяет и распределение легальной ренты, и структуру криминальных уязвимостей.

В этих условиях российско-китайское технологическое взаимодействие складывается как взаимодополняющая асимметрия. Уступая Пекину в масштабах электронной промышленности и вычислительной инфраструктуры, Россия компенсирует это фундаментальными научными школами, заделом в квантовых и криптографических технологиях, а главное — зрелой системой кибербезопасности и методиками расследования ИТ-преступлений, востребованными в рамках БРИКС, ШОС и СНГ.

Сопоставление страновых векторов доказывает, что пределы эффективности цифрового партнерства определяются качеством государственных институтов страны-партнера. Опыт Вьетнама свидетельствует, что при дееспособном государственном аппарате, столкнувшемся с давлением транснационального кибермошенничества, российское предложение успешно реализуется на стыке трансграничного доверенного документооборота и правоохранительной кооперации. Пример Венесуэлы демонстрирует обратную закономерность: создание непрозрачных цифровых и криптовалютных контуров обхода санкций при слабых институтах и криминализации государственного аппарата ведет к перехвату этой инфраструктуры организованной преступностью и генерирует для России прямые правовые и репутационные издержки.

Практическое значение этих выводов состоит в трех императивах: обязательной предварительной криминологической экспертизе институтов зарубежных цифровых партнеров; оценке эффективности цифровой дипломатии по ее вкладу в снижение трансграничной киберпреступности; приоритетной модернизации национального права в части перехода на постквантовую криптографию, уголовно-правовой квалификации деяний с использованием ИИ и пресечения легализации преступных доходов через криптоактивы. В теоретическом плане это ставит задачу сформировать на стыке международного права и криминологии направление, предметом которого выступает влияние правовых режимов цифровой среды на динамику и географию преступности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Лунеев В.В. Преступность XX века: мировые, региональные и российские тенденции / В.В. Лунеев. — 2-е изд., перераб. и доп. — Москва : Волтерс Клувер, 2005. — 912 с.

2. Крылов В.В. Информационные компьютерные преступления : учеб. и практ. пособие / В.В. Крылов. — Москва : Инфра-М, 1997. — 285 с.

3. Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина. — EDN OYYFEN // Криминология: вчера, сегодня, завтра. — 2012. — № 1 (24). — С. 45–55.

4. Овчинский В.С. Криминология цифрового мира : учебник / В.С. Овчинский. — 2-е изд., доп. и перераб. — Москва : Норма, 2026. — 348 с.

5. Жданов Ю.Н. Кибермафия. Мировые тенденции и международное противодействие : монография / Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский. — Москва : Норма, 2022. — 184 с.

6. Farrell H. Weaponized Interdependence: How Global Economic Networks Shape State Coercion / H. Farrell, A.L. Newman. — DOI 10.1162/isec_a_00351 // International Security. — 2019. — Vol. 44, no. 1. — P. 42–79.

7. Ларина Е.С. Кибервойны XXI века: о чем умолчал Эдвард Сноуден / Е.С. Ларина, В.С. Овчинский. — Москва : Книжный мир, 2014. — 352 с.

8. Hoffmann S. Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet / S. Hoffmann, D. Lazanski, E. Taylor. — DOI 10.1080/23738871.2020.1805482 // Journal of Cyber Policy. — 2020. — Vol. 5, no. 2. — P. 239–264.

9. Pohle J. Digital Sovereignty / J. Pohle, T. Thiel. — DOI 10.14763/2020.4.1532 // Internet Policy Review. — 2020. — Vol. 9, no. 4. — P. 1–19.

10. Arms Race or Innovation Race? Geopolitical AI Development / S. Schmid, D. Lambach, C. Diehl, C. Reuter. — DOI 10.1080/14650045.2025.2456019 // Geopolitics. — 2025. — Vol. 30, no. 4. — P. 1907–1936.

11. Fu X. Redefining China's Approach to AI Governance: Beyond Top-Down, Government-Led, and Command-and-Control / X. Fu, T. Huang. — DOI 10.1080/10670564.2026.2733081 // Journal of Contemporary China. — 2026.

12. Cantero Gamito M. The Influence of China in AI Governance Through Standardisation / M. Cantero Gamito. — DOI 10.1016/j.telpol.2023.102673 // Telecommunications Policy. — 2023. — Vol. 47, no. 10. — Art. 102673.

13. Criminal Networks in a Digitised World: On the Nexus of Borderless Opportunities and Local Embeddedness / E.R. Leukfeldt, E.R. Kleemans, E.W. Kruisbergen, R.A. Roks. — DOI 10.1007/s12117-019-09366-7 // Trends in Organized Crime. — 2019. — Vol. 22, no. 3. — P. 324–345.

14. Гришина В.Б. Международное сотрудничество стран БРИКС в сфере искусственного интеллекта как фактор обеспечения технологического суверенитета / В.Б. Гришина, М.Ю. Шерешева. — DOI 10.55959/MSU2070-1381-116-2026-112-123. — EDN TSXTAT // Государственное управление. Электронный вестник. — 2026. — № 116. — С. 112–123.

15. Овчинский В.С. Россия и вызовы цифровой среды : рабочая тетрадь / В.С. Овчинский, Е.С. Ларина, С.А. Кулик. — Москва : Спецкнига, 2014. — 40 с. — EDN YNZHZB.

16. Стрельцов А.А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности / А.А. Стрельцов. — EDN XVLADB // Международная жизнь. — 2017. — № 2. — С. 87–106.

17. Булва В.И. Международная информационная безопасность: от классической к сетевой дипломатии России / В.И. Булва. — DOI 10.21638/spbu06.2024.306. — EDN WDYACN // Вестник Санкт-Петербургского университета. Международные отношения. — 2024. — Т. 17, № 3. — С. 325–341.

18. Зиновьева Е.С. Международное управление Интернетом: конфликт и сотрудничество : учеб. пособие / Е.С. Зиновьева. — Москва : МГИМО-Университет, 2011. — 169 с. — EDN PXWVEJ.

19. Mapping the Global Geography of Cybercrime with the World Cybercrime Index / M. Bruce, J. Lusthaus, R. Kashyap [et al.]. — DOI 10.1371/journal.pone.0297312 // Plos One. — 2024. — Vol. 19, no. 4. — Art. e0297312.

20. Долгова А.И. Преступность, ее организованность и криминальное общество / А.И. Долгова. — Москва : Рос. криминол. ассоц., 2003. — 572 с.

21. Хыонг Тхы Хоанг. Цифровая экономика и электронная коммерция как новый вектор внешнеэкономических связей Вьетнама / Хыонг Тхы Хоанг. — DOI 10.64545/2072-8042-2026-2-95-112. — EDN JRLETZ // Российский внешнеэкономический вестник. — 2026. — № 2. — С. 95–112.

22. Канаев Е.А. Искусственный интеллект в деятельности вьетнамских стартапов как инструмент цифровой поддержки экономической интеграции АСЕАН / Е.А. Канаев. — DOI 10.54631/VS.2025.94-690533. — EDN ZQSKGF // Вьетнамские исследования. — 2025. — Т. 9, № 4. — С. 47–59.

23. Van Nguyen T. The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam / T. Van Nguyen. — DOI 10.1007/s12117-021-09422-1 // Trends in Organized Crime. — 2022. — Vol. 25, no. 2. — P. 226–247.

24. Luong H.T. "Simple job, high salary": Unveiling the Complexity of Scam-Forced Criminality in Southeast Asia / H.T. Luong. — DOI 10.1057/s41599-025-05605-1 // Humanities and Social Sciences Communications. — 2025. — Vol. 12. — Art. 1305.

25. Luong H.T. Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective / H.T. Luong, H.M. Ngo. — DOI 10.3390/laws13060070 // Laws. — 2024. — Vol. 13, no. 6. — Art. 70.

26. Ефремова И.А. Криминологическая характеристика компьютерной преступности и новые методы ее предупреждения / И.А. Ефремова. — DOI 10.17803/1729-5920.2025.222.5.077-086. — EDN ORCOTH // Lex russica. — 2025. — Т. 78, № 5 (222). — С. 77–86.

27. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е.А. Русскевич. — 2-е изд., перераб. и доп. — Москва : Инфра-М, 2022. — 351 с. — DOI 10.12737/1840963. — EDN MPWWHL.

28. Mantilla J.A. State-Crime Cooperation and Extra-legal Governance in Colombia and Venezuela / J.A. Mantilla. — DOI 10.1111/dech.70061 // Development and Change. — 2026. — Vol. 57, no. 3. — P. 599–623.

29. Bull B. From Bolibourgeoisie to Cryptocrats: How the Crisis and Sanctions Reshaped Venezuela's Ruling Elite into a New Oligarchy / B. Bull. — DOI 10.1080/01436597.2026.2633287 // Third World Quarterly. — 2026. — P. 1–21.

30. Rosales A. The Political Economy of Cryptocurrency in Latin America / A. Rosales. — DOI 10.1080/03085147.2026.2683279 // Economy and Society. — 2026. — P. 1–24.

31. Сидоренко Э.Л. Легализация преступных доходов с использованием DeFi: типовые схемы и индикаторы риска / Э.Л. Сидоренко. — DOI 10.21202/2782-2923.2023.4.822-836. — EDN DUPSPN // Russian Journal of Economics and Law. — 2023. — Т. 17, № 4. — С. 822–836.

32. Baradziej S. Harvest Now, Decrypt Later as a Cross-Sector Threat: A Scoping Review of Data-Confidentiality Lifetimes Against Post-Quantum Migration Readiness / S. Baradziej // International Journal of Computational Intelligence Systems. — 2026. — URL: https://doi.org/10.1007/s44196-026-01526-2.

33. Threat of Deepfakes to the Criminal Justice System: A Systematic Review / M.-P. Sandoval, M. de Almeida Vau, J. Solaas, L. Rodrigues. — DOI 10.1186/s40163-024-00239-1 // Crime Science. — 2024. — Vol. 13. — Art. 41.

34. Бегишев И.Р. Искусственный интеллект и уголовный закон : монография / И.Р. Бегишев, З.И. Хисамова. — Москва : Проспект, 2021. — 192 с. — EDN DZCJKJ.

35. Ларина Е.С. Искусственный интеллект. Большие данные. Преступность / Е.С. Ларина, В.С. Овчинский. — Москва : Книжный мир, 2018. — 416 с.

36. Foley S. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? / S. Foley, J.R. Karlsen, T.J. Putniņš. — DOI 10.1093/rfs/hhz015 // Review of Financial Studies. — 2019. — Vol. 32, no. 5. — P. 1798–1853.

37. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С.В. Иванцов, Э.Л. Сидоренко, Б.А. Спасенников [и др.]. — DOI 10.17150/2500-4255.2019.13(1).85-93. — EDN HRIXOZ // Всероссийский криминологический журнал. — 2019. — Т. 13, № 1. — С. 85–93.

38. Сидоренко Э.Л. Криптовалюта как предмет хищения: проблемы квалификации / Э.Л. Сидоренко. — EDN URLVIC // Мировой судья. — 2018. — № 6. — С. 18–24.

39. Lavorgna A. Criminal Markets and Networks in Cyberspace / A. Lavorgna, G.A. Antonopoulos. — DOI 10.1007/s12117-022-09450-5 // Trends in Organized Crime. — 2022. — Vol. 25, no. 2. — P. 145–150.

40. Овчинский В.С. Технологии будущего против криминала / В.С. Овчинский. — Москва : Книжный мир, 2017. — 288 с.

REFERENCES

1. Luneev V.V. *Criminality of the XX Century: World, Regional and Russian Tendencies*. 2nd ed. Moscow, Volters Kluver Publ., 2005. 912 p.

2. Krylov V.V. *Information Computer Crimes.* Moscow, Infra-M Publ., 1997. 285 p.

3. Nomokonov V.A., Tropina T.L. Cybercrime as a New Criminal Threat. *Kriminologiya: vchera, segodnya, zavtra = Criminology: Yesterday, Today, Tomorrow*, 2012, no. 1, pp. 45–55. (In Russian). EDN: OYYFEN.

4. Ovchinskii V.S. *Criminology of the Digital World*. 2nd ed. Moscow, Norma Publ., 2026. 348 p.

5. Zhdanov Yu.N., Kuznetsov S.K., Ovchinskii V.S. *Cyber-Mafia. Global Trends and International Counteraction.* Moscow, Norma Publ., 2022. 184 p.

6. Farrell H., Newman A.L. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 2019, vol. 44, no. 1, pp. 42–79. DOI: 10.1162/isec_a_00351.

7. Larina E.S., Ovchinskii V.S. *Cyberwars of the 21st Century: What Eduard Snowden did not Say.* Moscow, Knizhnyi Mir Publ., 2014. 352 p.

8. Hoffmann S., Lazanski D., Taylor E. Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy*, 2020, vol. 5, no. 2, pp. 239–264. DOI: 10.1080/23738871.2020.1805482.

9. Pohle J., Thiel T. Digital Sovereignty. *Internet Policy Review*, 2020, vol. 9, no. 4, pp. 1–19. DOI: 10.14763/2020.4.1532.

10. Schmid S., Lambach D., Diehl C., Reuter C. Arms Race or Innovation Race? Geopolitical AI Development. *Geopolitics*, 2025, vol. 30, no. 4, pp. 1907–1936. DOI: 10.1080/14650045.2025.2456019.

11. Fu X., Huang T. Redefining China's Approach to AI Governance: Beyond Top-Down, Government-Led, and Command-and-Control. *Journal of Contemporary China*. 2026. DOI: 10.1080/10670564.2026.2733081.

12. Cantero Gamito M. The Influence of China in AI Governance Through Standardisation. *Telecommunications Policy*, 2023, vol. 47, no. 10, art. 102673. DOI: 10.1016/j.telpol.2023.102673.

13. Leukfeldt E.R., Kleemans E.R., Kruisbergen E.W., Roks R.A. Criminal Networks in a Digitised World: On the Nexus of Borderless Opportunities and Local Embeddedness. *Trends in Organized Crime*, 2019, vol. 22, no. 3, pp. 324–345. DOI: 10.1007/s12117-019-09366-7.

14. Grishina V.B., Sheresheva M.Yu. International Cooperation of the Brics Countries in the Field of Artificial Intelligence as a Factor in Ensuring Technological Sovereignty. *Gosudarstvennoe upravlenie. Elektronnyi vestnik = Public Administration. E-Journal*, 2026, no. 116, pp. 112–123. (In Russian). EDN: TSXTAT. DOI: 10.55959/MSU2070-1381-116-2026-112-123.

15. Ovchinskii V.S., Larina E.S., Kulik S.A. *Russia and Challenges of Digital Environment.* Moscow, Spetskniga Publ., 2014. 40 p. EDN: YNZHZB.

16. Strel'tsov A.A. Sovereignty and Jurisdiction in the Environment of Information and Communication Technologies in the Context of International Security. *Mezhdunarodnaya zhizn' = International Affairs*, 2017, no. 2, pp. 87–106. (In Russian). EDN: XVLADB.

17. Bulva V.I. International Information Security: From Classical Towards Network Diplomacy in Russia. *Vestnik Sankt-Peterburgskogo universiteta. Mezhdunarodnye otnosheniya = Vestnik of Saint Petersburg University. International Relations*, 2024, vol. 17, no. 3, pp. 325–341. (In Russian). EDN: HKQPTD. DOI: 10.21638/spbu06.2024.306.

18. Zinov'eva E.S. *International Governance of the Internet: Conflict and Cooperation.* Moscow, MGIMO University Publ., 2011. 169 p. EDN: PXWVEJ.

19. Bruce M., Lusthaus J., Kashyap R., Phair N., Federico V. Mapping the Global Geography of Cybercrime with the World Cybercrime Index. *Plos One*, 2024, vol. 19, no. 4, art. e0297312. DOI: 10.1371/journal.pone.0297312.

20. Dolgova A.I. *Crime, its Organization and the Criminal Community.* Moscow, Russian Criminological Association Publ., 2003. 572 p.

21. Hoang H.T. Digital Economy and E-Commerce as a New Vector of Vietnam's Foreign Economic Relations. *Rossiiskii vneshneekonomicheskii vestnik = Russian Foreign Economic Journal*, 2026, no. 2, pp. 95–112. (In Russian). EDN: JRLETZ. DOI: 10.64545/2072-8042-2026-2-95-112.

22. Kanaev E.A. Artificial Intelligence in the Activities of Vietnamese Startups as a Tool for Digital Support of the Asean-Led Economic Integration. *V'etnamskie Issledovaniya: Ehlektronnyi Nauchnyi Zhurnal = Russian Journal of Vietnamese Studies*, 2025, vol. 9, no. 4, pp. 47–59. (In Russian). EDN: ZQSKGF. DOI: 10.54631/VS.2025.94-690533.

23. Van Nguyen T. The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam. *Trends in Organized Crime*, 2022, vol. 25, no. 2, pp. 226–247. DOI: 10.1007/s12117-021-09422-1.

24. Luong H.T. "Simple job, high salary": Unveiling the Complexity of Scam-Forced Criminality in Southeast Asia. *Humanities and Social Sciences Communications*, 2025, vol. 12, art. 1305. DOI: 10.1057/s41599-025-05605-1.

25. Luong H.T., Ngo H.M. Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective. *Laws*, 2024, vol. 13, no. 6, art. 70. DOI: 10.3390/laws13060070.

26. Efremova I.A. Criminological Characterization of Computer Crime and New Methods of Its Prevention. *Lex russica*, 2025, vol. 78, no. 5, pp. 77–86. (In Russian). EDN: ORCOTH. DOI: 10.17803/1729-5920.2025.222.5.077-086.

27. Russkevich E.A. *Criminal Law and "Digital Crime": Problems and Solutions*. 2nd ed. Moscow, Infra-M Publ., 2022. 351 p. EDN: MPWWHL. DOI: 10.12737/1840963.

28. Mantilla J.A. State-Crime Cooperation and Extra-Legal Governance in Colombia and Venezuela. *Development and Change*, 2026, vol. 57, no. 3, pp. 599–623. DOI: 10.1111/dech.70061.

29. Bull B. From Bolibourgeoisie to Cryptocrats: How the Crisis and Sanctions Reshaped Venezuela's Ruling Elite into a New Oligarchy. *Third World Quarterly*, 2026, pp. 1–21. DOI: 10.1080/01436597.2026.2633287.

30. Rosales A. The Political Economy of Cryptocurrency in Latin America. *Economy and Society*, 2026, pp. 1–24. DOI: 10.1080/03085147.2026.2683279.

31. Sidorenko E.L. Legalization of Criminal Income Using Defi: Typical Schemes and Risk Indicators. *Russian Journal of Economics and Law*, 2023, vol. 17, no. 4, pp. 822–836. (In Russian). EDN: DUPSPN. DOI: 10.21202/2782-2923.2023.4.822-836.

32. Baradziej S. Harvest Now, Decrypt Later as a Cross-Sector Threat: A Scoping Review of Data-Confidentiality Lifetimes Against Post-Quantum Migration Readiness. *International Journal of Computational Intelligence Systems*, 2026. Available at: https://doi.org/10.1007/s44196-026-01526-2.

33. Sandoval M.-P., Vau M. de Almeida, Solaas J., Rodrigues L. Threat of Deepfakes to the Criminal Justice System: A Systematic Review. *Crime Science*, 2024, vol. 13, art. 41. DOI: 10.1186/s40163-024-00239-1.

34. Begishev I.R., Khisamova Z.I. *Artificial Intelligence and Criminal Law*. Moscow, Prospekt Publ., 2021. 192 p. EDN: DZCJKJ.

35. Larina E.S., Ovchinskii V.S. *Artificial Intelligence. Big Data. Crime.* Moscow, Knizhnyi Mir Publ., 2018. 416 p.

36. Foley S., Karlsen J.R., Putniņš T.J. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies*, 2019, vol. 32, no. 5, pp. 1798–1853. DOI: 10.1093/rfs/hhz015.

37. Ivantsov S.V., Sidorenko E.L., Spasennikov B.A., Berezkin Yu.M., Sukhodolov Ya.A. Cryptocurrency-Related Crimes: Key Criminological Trends. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 1, pp. 85–93. (In Russian). EDN: HRIXOZ. DOI: 10.17150/2500-4255.2019.13(1).85-93.

38. Sidorenko E.L. Cryptocurrency as a Subject of Embezzlement: Qualification Issues. *Mirovoi sud'ya = Justice of the Peace*, 2018, no. 6, pp. 18–24. (In Russian). EDN: URLVIC.

39. Lavorgna A., Antonopoulos G.A. Criminal Markets and Networks in Cyberspace. *Trends in Organized Crime*, 2022, vol. 25, no. 2, pp. 145–150. DOI: 10.1007/s12117-022-09450-5.

40. Ovchinskii V.S. *Technologies of the Future against Crime.* Moscow, Knizhnyi Mir Publ., 2017. 288 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Сидоренко Элина Леонидовна — доктор юридических наук, профессор Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации, 119454, Российская Федерация, г. Москва, пр-кт Вернадского, 76, 12011979@list.ru, https://orcid.org/0000-0002-4741-0184, СПИН-код: 3744-0382.

INFORMATION ABOUT THE AUTHOR

Sidorenko, Elina L. — Doctor of Law, Professor, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation, 76 Vernadsky Ave., Moscow, 119454, the Russian Federation, 12011979@list.ru, https://orcid.org/0000-0002-4741-0184, SPIN-Code: 3744-0382.